Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Comprehension of cyber threats and their consequences in Slovenia

Blaž Markelj, Sabina Zgaga *

Faculty of Criminal Justice and Security, University of Maribor, Ljubljana, Slovenia

Keywords:
Cyber threats
Mobile devices
Awareness
Criminal responsibility
Guilt

A B S T R A C T

Mobile devices are used more and more frequently. We discovered that students do not use their mobile devices just for private purposes but also for work related tasks; furthermore, they use their private mobile devices to access various information systems and corporate data that can be classified, or marked as trade secrets, personal data or professional secrecy. Individuals who are granted authorised access to these types of data are obliged to protect them from unauthorised access and cyber threats. In our survey, we tried to find out how well students were aware of the existing information security threats to mobile devices and to the data which they access through mobile devices. The results of our survey and criminal law analysis have shown us that the student population is not well aware of security threats and security measures. Because the user of a mobile device can be held criminally responsible for the loss of data that he or she had accessed by using the mobile device, even though he or she is not aware of security threats and protective measures against them, we believe that it will be necessary to encourage users to educate themselves about the new cyber threats that are typically targeting mobile devices, and also to familiarise themselves with the methods of protecting their mobile devices. To this purpose, organisations should implement internal regulations and continuously educate mobile device users about their safe usage in accordance with organisational standards.

1. Comprehension of cyber threats and their consequences

1.1. *Introduction – theoretical basis*

Information technology has become a necessary element of our everyday lives because it enables us to communicate and work faster, more efficiently and with greater ease. The continually quickening pace of life has also created a need for constant access to cyberspace, and this is possible because of increasingly sophisticated technological solutions. We are experiencing a great expansion of the World Wide Web (WWW), which we can now access through various devices. Between 2000 and 2009, the WWW has expanded by 380% (Schjolberg, 2010). To access the Web we had, until recently, relatively simple stationary computers; now these are rapidly being replaced by mobile devices. Mobile devices mostly include devices with an adapted operational system, such as iOS, Android, BlackBerry OS, Windows mobile; and are portable (mobile phones, tablets, etc.). This category can include all portable devices with a wireless Internet access (including laptops, portable gaming consoles, industrial readers, etc.). On the other hand, the mobile phone group includes both mobiles phones intended solely for phone calls and sending short messages and smart mobile phones representing a modern communication device, which offers a whole range of additional functions, similar to those of a personal computer, in addition to calls through mobile networks.

* Corresponding author. Faculty of Criminal Justice and Security, University of Maribor, Kotnikova 8, 1000 Ljubljana, Slovenia.
E-mail address: sabinazgaga@gmail.com (S. Zgaga).

http://dx.doi.org/10.1016/j.clsr.2016.01.006

According to the Microsoft Tag (2011) report, soon more people will be using mobile devices to access the Internet than stationary computers. At the time we are writing this, the ratio between mobile and stationary Internet connections is 50:50. To establish a wireless connection to the Internet, one needs a mobile device – currently, smart mobile phones are the most popular. The research efforts of IDC (2011) showed that a 55% global increase of mobile device users per year can be expected. A report by IDC (2014), showing sales of smart mobile phones (these belong to the group of mobile device), says that only in 2013, sales of these devices exceeded one billion units. In this respect, Slovenia is not lagging behind; quite the contrary, the findings of the CEE Telco Industry Report carried out by GfKGroup (2011) in 15 Eastern-European countries were that Slovenia is in top place – 27.8% users of mobile telecommunications have smartphones.

The results of the Ponemon survey (Ponemon, 2011), which was carried out with the purpose of determining how well users of smart mobile phones in the USA were aware of privacy and information security issues, showed that people did in fact quite frequently use these devices to transfer various data from the Internet. It was also interesting to find out that most mobile smartphone users used their device for both personal and business purposes. On average, a US citizen spends 2.7 hours a day connected to social networks or communicating via some type of mobile device (Microsoft Tag, 2011).

For younger generations, being more or less constantly 'connected' has become a necessity. Only rare individuals still do not have their personal profile on the Internet and have no virtual friends. Friendships are maintained through communication, be it in cyberspace or in reality. Mobile devices are tools for establishing and maintaining contact with the cyber-community.

Young users often perceive security measures designed to protect data as a nuisance or obstacle to communication. They particularly like the possibility to be continually online and in contact with their friends via messaging or through social networks such as Facebook, Google Chat, Twitter, etc. The development of software for mobile devices is extremely rapid, most certainly so to attract youth and increase sales. Young users of mobile devices often forget about all the potential security traps and threats in cyberspace and do not use adequate protection. Accordingly, Ponemon (2012) published in December 2012 the results of a research on mobility risk in organisations regarding the mobile devices and also the information infrastructure used by users; 70% of the respondents chose mobile devices as the biggest risk for the safety of information technology. For comparison; in 2010 only 9% of the respondents and in 2011 only 48% of the respondents chose mobile devices. Further, the respondents recognised mobile devices as the second biggest risk in 2012 across 3rd party applications (67% of the respondents). This clearly shows a continuing growth of those respondents, who comprehend mobile devices not only as a useful means for work but also as a threat to information technology and systems of organisations, if not handled properly.

It is important to be aware of various threats in cyberspace and the consequences these can have for mobile device users, since this affects general information security and efforts to maintain it. Some security measures are rather obvious and commonly known (e.g., PIN-code for SIM-cards, locking Bluetooth connections and mobile devices), while others are less so, and users have to be appropriately informed about them. After all, we hear news of new models of mobile devices and software all the time.

Mobile devices can be the target of software fragments downloaded to a device with the help of malicious software, such as malware, spyware, and Botnet, or through the Bluetooth module when a user is connected to a social network (Leavitt, 2011). The results of a survey carried out by Lookout (2011) showed that in the second half of 2011, the number of malware threats increased by 14%, compared to spyware threats. There is a possibility that 1 to 4% of mobile devices get infected by malware. Juniper's (2011) report states that from the summer of 2010, the number of mobile devices running on the Android platform infected with malware had increased by 400%. In the same report, we can read that 85% of mobile users do not use efficient protection for their mobile devices. Providers of software for mobile devices take the liberty of installing 'back doors' or programs that manage settings on the mobile device, automatically send data about the user's location (GPS) and can take control of the mobile device, all without the user's knowledge. Also in Juniper (2013), there were again reports on a great increase in threats to mobile devices. This report was based on one year continuous observation of the development and existence of threats to mobile devices. Accordingly, the mobile malware threats grew at a rapid rate of 614% between March 2012 and 2013, whereas 73% of all known malware are Fake Installers or SMS Trojans, which exploit holes in mobile payments to make a quick and easy profit. The trend of growing threats to mobile devices continues in 2014 as well, according to McAfee (2014). Users who are unaware of the potential dangers of (malicious) software for mobile devices can become the target of cyber criminals and encounter serious problems.

Meško and Bernik (2011) describe cyber criminality as a concept that is still not well understood by the general public, but they outlined a definition of cyber-crime based on the theoretical findings of other authors (Alshalan, 2011; Završnik, 2005) and the International Convention on Cyber Crime. According to Meško and Bernik, '. . . cyber-crime is the use of information and communication technology to perpetrate criminal acts'. It should be emphasised that cyber-crime also comprises malicious and immoral acts in cyberspace which are not necessarily penalised (Dimc and Dobovšek, 2010). The previously mentioned authors furthermore state that, '. . . some types of cybercrimes are so common that they have become socially accepted, e.g., piracy'. In the Threat Assessment Report issued by Europol (2011), we can read that 'data mobility' is one of the reasons why there are now more opportunities for cyber criminals. Data mobility became possible because of mobile devices. As we have already determined, the number of mobile device users is steadily growing. Mobile devices are difficult to monitor and protect precisely because of their mobility, but not trying to do so means that one can easily become the target and victim of cyber criminals.

In December 2011, a survey titled *Awareness of the Threats to Mobile Devices amongst Youth* was conducted among Slovenian students. Its purpose was to find out how well young users of mobile devices are aware of the threats and dangers they are exposed to in cyberspace and which types of security